

INDEX

	Page
Opinions below-----	1
Jurisdiction-----	1
Questions presented-----	2
Constitutional provision and statute involved-----	2
Statement-----	2
Summary of Argument-----	5
Argument-----	9
I. An electronic surveillance that the Attorney General has authorized as necessary to pro- tect the national security is not an unrea- sonable search and seizure under the Fourth Amendment solely because it is conducted without prior judicial approval-----	9
A. The determination whether a search and seizure is reasonable under the Fourth Amendment requires a weighing of the competing in- terests involved-----	11
B. When the governmental interest in protecting national security is bal- anced against the invasion of per- sonal rights resulting from elec- tronic surveillance, the proper con- clusion is that a warrant is not re- quired, before such surveillance may be made-----	15

(1)

Argument—Continued

Page

I. An electronic surveillance etc.—Continued

B. When the governmental interest etc.—Continued

1. The President has a duty to protect the national security and he has authority to gather intelligence information necessary to perform that function.....

15

2. The Attorney General, acting on behalf of the President, may authorize surveillance in national security cases.....

19

a. In authorizing such surveillance the Attorney General properly acts on behalf of the President.....

19

b. The standard of national security that the Attorney General applies is the same standard Congress provided in the Omnibus Crime Control and Safe Streets Act of 1968.....

20

c. The Attorney General's action in authorizing the surveillance is subject to limited judicial review.....

21

3. The Fourth Amendment does not require a warrant for a national security electronic surveillance that the Attorney General has authorized.....

23

Argument—Continued

Page

I. An electronic surveillance etc.—Continued

B. When the governmental interest etc.—Continued

3. The Fourth Amendment etc.
Continued

a. Requiring a warrant in national security electronic surveillance is likely to frustrate the governmental purpose of such surveillance ----- 23

b. Congress has recognized the Attorney General's authority to authorize national security electronic surveillance without a warrant ----- 28

c. The considerations involved in authorizing national security surveillance are so interrelated to those involved in conducting foreign intelligence operations, and the two activities are so interrelated, that it would be inappropriate to impose stricter standards for the former than for the latter ----- 30

d. The possibility that the Attorney General could abuse his power to authorize national security electronic surveillance without a warrant is not a valid reason for denying him that power ----- 35

Argument—Continued

- II. If it is determined that electronic surveillance to protect national security is unlawful in the absence of prior judicial authorization, courts should be permitted to determine *in camera* whether illegal interceptions are arguably relevant to a prosecution before requiring their disclosure to the defendant.

Conclusion

Appendix

Page

35

47

48

CITATIONS

Cases:

<i>Abel v. United States</i> , 362 U.S. 217	12
<i>Agnello v. United States</i> , 269 U.S. 20	
<i>Alderman v. United States</i> , 394 U.S. 165	2,
	8, 36, 37, 46
<i>Alexander v. United States</i> , 362 F. 2d 379, <i>certiorari denied</i> , 385 U.S. 977	12
<i>Anderson v. Dunn</i> , 6 Wheat 204	
<i>Anderson v. Sills</i> , 56 N.J. 210, 265 A. 2d 678	14
<i>Aptheker v. Secretary of State</i> , 378 U.S. 500	26
<i>Barenblatt v. United States</i> , 360 U.S. 109	7
<i>Barrett v. Kunzig</i> , Civ. No. 6193, M.D. Tenn., decided August 11, 1971	12, 18
<i>Boyd v. United States</i> , 116 U.S. 616	12
<i>Brownell v. Rasmussen</i> , 235 F. 2d 527, <i>certiorari dismissed</i> , 355 U.S. 859	20
<i>Cafeteria Workers v. McElroy</i> , 367 U.S. 886	16
<i>Camara v. Municipal Court</i> , 387 U.S. 523	6,
	11-12, 14
<i>Carroll v. United States</i> , 267 U.S. 132	12
<i>Chambers v. Maroney</i> , 399 U.S. 42	12
<i>Chicago & Southern Air Lines, Inc. v. Waterman Steamship Corp.</i> , 333 U.S. 103	16, 13

Cases—Continued

	Page
<i>Chimel v. California</i> , 395 U.S. 752.....	12
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443.....	19
<i>Cooper v. California</i> , 386 U.S. 58.....	12
<i>Cox v. New Hampshire</i> , 312 U.S. 569.....	14
<i>Dakota Central Telephone v. South Dakota</i> , 250 U.S. 163.....	32
<i>Giordano v. United States</i> , 394 U.S. 310.... 11, 23, 37	
<i>In re Debs</i> , 158 U.S. 564.....	16
<i>Johnson v. Eisentrager</i> , 339 U.S. 763.....	32
<i>Katz v. United States</i> , 389 U.S. 347.... 11, 13, 14, 20	
<i>Knauff v. Shaughnessy</i> , 338 U.S. 537.....	20
<i>McDonald v. United States</i> , 335 U.S. 451.....	12
<i>Murray's Lessee v. Hoboken Land Improvement Co.</i> , 18 Howard 272.....	12
<i>Myers v. United States</i> , 272 U.S. 52.....	20
<i>Olmstead v. United States</i> , 277 U.S. 438.....	11
<i>Oetjen v. Central Leather Co.</i> , 246 U.S. 297.... 16, 32	
<i>Prize Cases</i> , 2 Black 635.....	32
<i>Roviaro v. United States</i> , 353 U.S. 53.....	37
<i>Schmerber v. California</i> , 384 U.S. 757.....	12
<i>Stanley v. Georgia</i> , 394 U.S. 557.....	11
<i>Taglianetti v. United States</i> , 394 U.S. 316.... 37, 44	
<i>Terry v. Ohio</i> , 392 U.S. 1.....	12, 13
<i>Totten v. United States</i> , 92 U.S. 105.....	16, 39
<i>United States v. Belmont</i> , 301 U.S. 324.....	16, 32
<i>United States v. Butenko and Ivanov</i> , No. 418- 63, D.J.N., decided October 13, 1970.....	33
<i>United States v. Clay</i> , 430 F.2d 165, certiorar: granted and reversed on another issue.... 30, 32	
<i>United States v. Curtiss-Wright Corp.</i> , 299 U.S. 304.....	16, 31
<i>United States v. Dellinger, et al.</i> , Cr. No. 69-180, N.D. Ill., E.D., decided February 20, 1970.....	33

Cases—Continued

<i>United States v. Hogans</i> , 369 F.2d 359	32
<i>United States v. Johnson</i> , 425 F. 2d 630	12
<i>United States v. Midwest Oil Co.</i> , 236 U.S. 459	18
<i>United States v. O'Baugh</i> , 304 F.Supp. 767	33
<i>United States v. Pink</i> , 315 U.S. 203	16, 32
<i>United States v. Reynolds</i> , 345 U.S. 1	39
<i>United States v. Robel</i> , 389 U.S. 258	26
<i>United States v. Stone</i> , 305 F.Supp. 75	33
<i>United States v. White</i> , 401 U.S. 745	23
<i>Walker v. United States</i> , 404 F.2d 900	12
<i>Warden v. Hayden</i> , 387 U.S. 294	12
<i>Wyman v. James</i> , 400 U.S. 309	12
Constitution, statutes and rule:	
United States Constitution:	
Article II, Section 1	15
Fourth Amendment	<i>passim</i>
Omnibus Crime Control and Safe Streets Act of 1968 (82 Stat. 197, 18 U.S.C. 2510 <i>et</i> <i>seq.</i>)	
18 U.S.C. 2510-2520	41, 43
18 U.S.C. 2511(3)	21, 34, 41, 48
18 U.S.C. 2518 (8)	37, 41
18 U.S.C. 2518 (10)	37, 41
Organized Crime Control Act of 1970, 84 Stat. 922 <i>et seq.</i> (P.L. 91-452):	
18 U.S.C. 371	2
18 U.S.C. 1361	2
18 U.S.C. 3504 (Title VII)	37, 42
F. R. Crim. R., Rule 16(e)	38
Congressional material:	
115 Cong. Rec. S5810-5816 (daily ed., May 29, 1969)	45
116 Cong. Rec. S127-130 (daily ed., Jan. 19, 1970)	45

VII

Congressional material—Continued

	Page
116 Cong. Rec. S464-471 (daily ed., Jan. 23, 1970)-----	45
116 Cong. Rec. H9649 (daily ed., Oct. 6, 1970)-----	44
116 Cong. Rec. H9655 (daily ed., Oct. 6, 1970)-----	45
116 Cong. Rec. H9710-9711 (daily ed., Oct. 7, 1970)-----	44
116 Cong. Rec. H9721 (daily ed., Oct. 7, 1970)-----	45
116 Cong. Rec. H9730 (daily ed., Oct. 7, 1970)-----	45
116 Cong. Rec. S17775 (daily ed., Oct. 12, 1970)-----	46
Hearings before a Subcommittee of the Committee on Appropriations of the House of Representatives, 87th Cong., 2d Session (January 22, 1962)-----	27
Hearings before a Subcommittee of the Committee on Appropriations of the House of Representatives, 88th Cong. 1st Session (January 29, 1963)-----	27
Hearings before a Subcommittee of the Committee on Appropriations of the House of Representatives, 91st Cong., 2d Session (February 17, 1970)-----	27
Hearings before Subcommittee No 5 of the House Committee on the Judiciary on H.R. 762, 867, 4513, 4728 and 5096, on <i>Wiretapping</i> , 84th Cong., 1st Session (1955)-----	27
Hearings pursuant to S. Res. 234, before the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, on <i>Wiretapping, Eavesdropping, and the Bill of Rights</i> , 85th Cong., 2d Session (1958)-----	26

Congressional material—Continued

	Page
Hearings before the Senate Permanent Subcommittee on Investigations of the Committee on Government Operations, on <i>Riots and Civil and Criminal Disorder</i> , Exhibit 825, Part 25, 91st Cong., 2d Sess. (1970)-----	18
S. Rep. No. 91-617, 91st Cong., 2d Sess.-----	43
S. Rep. No. 1097, 90th Cong., 2d Sess.-----	29, 41
Miscellaneous:	
Brownell, <i>The Public Security and Wire Tapping</i> , 39 Cornell L.Q. 195-----	17, 25, 27
Connolly, Richard, <i>The Story of the Patriarca Transcripts</i> , Boston Evening Globe, September 2, 1971-----	44
<i>Life Magazine</i> , May 30, 1969-----	38
<i>Report of the Committee of Privy Councillors Appointed to Inquire Into the Interception of Communications</i> (1957)-----	28
Rogers, <i>The Case for Wire Tapping</i> , 63 Yale L.J. 792-----	17, 27
Statistics, National Bomb Data Center, Management and Research Division, International Ass'n of Chiefs of Police (1971)-----	18
Telford Taylor, <i>Two Studies in Constitutional Interpretation</i> (1969)-----	26, 27

In the Supreme Court of the United States

OCTOBER TERM, 1971

No. 70-153

UNITED STATES OF AMERICA, PETITIONER

v.

UNITED STATES DISTRICT COURT FOR THE EASTERN
DISTRICT OF MICHIGAN, SOUTHERN DIVISION AND
HONORABLE DAMON J. KEITH

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF
APPEALS FOR THE SIXTH CIRCUIT

BRIEF FOR THE UNITED STATES

OPINIONS BELOW

The opinions of the court of appeals (App. 33-85) and of the district court (App. 23-32) are not reported.

JURISDICTION

On April 8, 1971, the court of appeals denied the government's petition for a writ of mandamus seeking to compel the respondent district judge to vacate a pretrial order entered in a pending criminal case and the judgment of the court of appeals (App. 87) was entered on that same date. The petition for a writ of certiorari was filed on May 8, 1971, and was granted on June 21, 1971 (App. 88; 403 U.S. 930). The jurisdiction of this Court rests upon 28 U.S.C. 1254(1).

QUESTIONS PRESENTED

1. Whether electronic surveillance that the Attorney General authorized as necessary to protect the national security is an unreasonable search and seizure solely because it was conducted without prior judicial approval.¹

2. If such national security surveillances are unlawful, whether— notwithstanding *Alderman v. United States*, 394 U.S. 165—it would be appropriate for the district court to determine *in camera* whether the interceptions are arguably relevant to the prosecution before requiring their disclosure to the defendant.

CONSTITUTIONAL PROVISION AND STATUTE INVOLVED

The pertinent provisions of the Fourth Amendment to the Constitution and of the Omnibus Crime Control and Safe Streets Act of 1968 are set forth in the Appendix, *infra*.

STATEMENT

This case arises from a criminal proceeding, pending trial in the United States District Court for the Eastern District of Michigan, in which the three defendants are charged with conspiracy to destroy government property in violation of 18 U.S.C. 371, and one of the defendants, Plamondon, is charged with destruction of government property in violation of 18 U.S.C. 1361 (App. 5-7). The indictment resulted from the bombing of an office of the Central Intelligence Agency in Ann Arbor, Michigan (App. 6).

¹ This statement of the question is a narrowing of, but covered by, the first question presented in the petition.

During pretrial proceedings, the defendants filed a motion for disclosure of electronic surveillance information (App. 8-9, 23). With its response, the government filed and served upon the movants an affidavit of the Attorney General of the United States, acknowledging that government agents had overheard conversations participated in by Plamondon; it also filed the logs of these surveillances as a sealed exhibit (App. 34-35).²

The Attorney General's affidavit reads as follows:

JOHN N. MITCHELL being duly sworn deposes and says:

1. I am the Attorney General of the United States.

2. This affidavit is submitted in connection with the Government's opposition to the disclosure to the defendant Plamondon of information concerning the overhearing of his conversations which occurred during the course of electronic surveillances which the Government contends were legal.

3. The defendant Plamondon has participated in conversations which were overheard by Government agents who were monitoring wiretaps which were being employed to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government. The records of the Department of Justice reflect the installation of these wiretaps had been expressly approved by the Attorney General.

4. Submitted with this affidavit is a sealed exhibit containing the records of the inter-

² The sealed exhibit is part of the record before the Court.

cepted conversations, a description of the premises that were the subjects of the surveillances, and copies of the memoranda reflecting the Attorney General's express approval of the installation of the surveillances.

5. I certify that it would prejudice the national interest to disclose the particular facts concerning these surveillances other than to the court *in camera*. Accordingly, the sealed exhibit referred to herein is being submitted solely for the court's *in camera* inspection and a copy of the sealed exhibit is not being furnished to the defendants. I would request the court, at the conclusion of its hearing on this matter, to place the sealed exhibit in a sealed envelope and return it to the Department of Justice where it will be retained under seal so that it may be submitted to any appellate court that may review this matter. [App. 20-21]

On the basis of this affidavit and the sealed exhibit, the government asserted that the surveillances were lawful, though conducted without prior judicial approval, as a reasonable exercise of the President's power (exercised through the Attorney General) to utilize the investigative resources at his disposal to secure the intelligence necessary for the preservation of the national security (App. 25).

The district court (Judge Keith) rejected this argument, and held that the surveillance, because it had not received prior judicial sanction, violated the Fourth Amendment (App. 23-32). It ordered the

government to make full disclosure to Plamondon of his overheard conversations as a necessary prelude to an evidentiary hearing at the conclusion of the trial to determine whether any of the evidence upon which the indictment was based or which the government intends to offer at trial is "taint[ed]" by the surveillance (App. 32).

The government then filed in the court of appeals a petition for a writ of mandamus to set aside this order. The court of appeals denied the petition (App. 68). It agreed that the case was an appropriate one for mandamus, since the order was not appealable and raised "[g]reat issues * * * for all parties concerned" which were of first impression in any appellate court (App. 39). On the merits, the court (Judge Weick dissenting) held that the district court had properly found the surveillances unlawful under the Fourth Amendment, and had properly required disclosure of the overheard conversations (App. 40-64). The court rejected the government's alternative argument that even if the surveillances were illegal, the special circumstances of this case made appropriate an *in-camera* determination, without disclosure to the defendant, of its contention that the conversations intercepted were irrelevant to the prosecution (App. 64-68).

SUMMARY OF ARGUMENT

I.

The Fourth Amendment does not prohibit all searches and seizures without a warrant, but only unreasonable ones. The determination whether a par-

ticular search is reasonable requires "balancing the need to search against the invasion which the search entails." *Camara v. Municipal Court*, 387 U.S. 523, 537. We submit that an electronic surveillance authorized by the Attorney General as necessary to protect the national security is not an unreasonable search and seizure solely because it is conducted without prior judicial approval.

The President, as chief executive, is responsible for assuring that our system of government is a functioning, viable entity, and for safeguarding it against overthrow by unlawful means. As this Court has recognized, proper performance of this duty requires that the President have complete information concerning actual and potential threats to national security. For the past 30 years Presidents have authorized electronic surveillance in national security cases without a warrant, and the need therefor is equally great today.

In authorizing such surveillances, the Attorney General properly acts for the President. The standard the Attorney General applies is that Congress provided in the Omnibus Crime Control and Safe Streets Act of 1968. The Attorney General's authorization is subject to judicial review, to assure that his determination to make the surveillance was not arbitrary and capricious.

Requiring a warrant for national security electronic surveillance would frustrate the governmental purpose behind the surveillance. To obtain a warrant, the government would have to disclose sensitive and highly secret information, which would significantly re-

duce the chances of the surveillance being effective. Moreover, in determining whether a warrant should issue, a judge would be called upon to perform a function outside the traditional judicial responsibilities; the need for intelligence gathering ordinarily involves consideration of a large number of complicated facts and subtle inferences. Allowing the Attorney General to authorize such surveillances without prior approval by a magistrate would centralize responsibility on this matter, thereby promoting uniformity in the standards governing them and facilitating close control of use of this investigative technique.

The legislative history of the Omnibus Crime Control and Safe Streets Act of 1968 indicates that in excepting national security surveillances from the Act's warrant requirement Congress recognized the President's authority to conduct such surveillances without prior judicial approval. Moreover, a warrant is not required for surveillances conducted to gather foreign intelligence information. The reasoning that supports this conclusion applies equally to all national security matters: all such matters involve highly complex factors that make judicial scrutiny impracticable and no clear distinction can be drawn between foreign and domestic threats to the national security, as Congress itself has recognized in the 1968 Act. Finally, the possibility that the Attorney General might abuse his power to authorize surveillances of this sort is not a valid basis for denying him that power, since his acts would be subject to judicial review to protect against abuse.

II

If national security surveillances conducted without a warrant are, contrary to our contention, unlawful, we urge that the Court reconsider the automatic disclosure rule of *Alderman v. United States*, 394 U.S. 165. We submit that in this area courts should be permitted to make an initial *in camera* determination whether the information obtained by the surveillance is arguably relevant to a prosecution before turning the material over to a defendant.

Disclosure of overheard conversations has a serious potential for injury, to persons whose innocent conversations were overheard, to third persons mentioned in such conversations, to informants and their families, and to pending investigations and prosecutions. Moreover, as in this case, the defendant to whom disclosure must be made frequently is not the subject of surveillance and his overheard conversation bears no relation to his prosecution. The problems of automatic disclosure are especially troublesome in the national security area, where secrecy is essential to the success of the government's intelligence gathering operations. Automatic disclosure for national security cases would require the government to face an undesirable dilemma: either to drop the prosecution of an often serious crime or to reveal sensitive secret information.

The *Alderman* rule is most reasonably viewed as an exercise of the Court's supervisory powers. Congress has rejected automatic disclosure in favor of a more flexible approach in the Omnibus Crime Control and

Safe Streets Act of 1968, because of the special dangers that disclosure entails and because protective orders had proved insufficient to cope with those dangers. We believe that this enactment supplants the rule of *Alderman* in the circumstances to which it applies, and indicates a congressional intent that in the national security area, which the Act specifically excepts from its coverage, the *Alderman* rule should not be applied to interceptions after its effective date. This view is strengthened by the legislative history of Title VII of the Organized Crime Control Act of 1970, in which Congress explicitly overturned the *Alderman* rule for all cases arising prior to the effective date of the 1968 Act. In light of the strongly expressed congressional view that automatic disclosure is undesirable and not constitutionally required, we submit that that rule should not apply to the national security area.

ARGUMENT

I.

AN ELECTRONIC SURVEILLANCE THAT THE ATTORNEY GENERAL HAS AUTHORIZED AS NECESSARY TO PROTECT THE NATIONAL SECURITY IS NOT AN UNREASONABLE SEARCH AND SEIZURE UNDER THE FOURTH AMENDMENT SOLELY BECAUSE IT IS CONDUCTED WITHOUT PRIOR JUDICIAL APPROVAL

INTRODUCTION

The constitutional issue before the Court, although of great importance, is narrow: whether the fact that there has been no prior judicial approval of an elec-

tronic surveillance that the Attorney General has authorized as necessary to protect the national security necessarily and on that ground alone converts the surveillance into an unreasonable search and seizure that violates the Fourth Amendment. The government makes no claim that such authorization by the Attorney General itself establishes compliance with the Fourth Amendment standard of reasonableness; it urges the Court only to hold that the absence of prior judicial approval does not invalidate the search under that standard.

As we explain below (pp. 21-23), we recognize that the courts properly may review the action of the Attorney General in authorizing such surveillance. We argue, however, that the scope of such review is necessarily extremely limited, and that great deference must be given to the Attorney General's judgment that a particular surveillance is necessary to protect the national security.

There is no issue here of the authority of the government to engage in sweeping electronic surveillance without prior judicial approval as a general law enforcement technique. The government claims no authority to do that. Nor does it urge a broad definition of "national security" that could cover many or most criminal investigations. The standard it proposes here is the same standard that Congress adopted in the Omnibus Crime Control and Safe Streets Act of 1968, in authorizing electronic surveillance without a warrant. See, *infra*, pp. 20-21.

This Court has expressly left open the question

"[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security * * *" (*Katz v. United States*, 389 U.S. 347, 358, n. 23; see *Giordano v. United States*; 394 U.S. 310, 314-315). We urge the Court to adopt the principle that Mr. Justice White suggested in his concurring opinion in *Katz* (389 U.S. at 364): "We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable." That rule, we submit, properly would effectuate the basic principle that the Fourth Amendment prohibits only "unreasonable" searches and seizures, and would accord with the decisions of this Court defining the protection which that Amendment was intended to provide against arbitrary governmental invasions of "the right to be let alone" (Mr. Justice Brandeis, dissenting in *Olmstead v. United States*, 277 U.S. 438, 478, quoted with approval in *Stanley v. Georgia*, 394 U.S. 557, 564).

A. The Determination Whether a Search and Seizure is Reasonable Under the Fourth Amendment Requires a Weighing of the Competing Interests Involved.

"[T]here can be no ready test for determining reasonableness [under the Fourth Amendment] other than by balancing the need to search against the invasion which the search entails" (*Camara v. Municipi-*

pal Court, 387 U.S. 523, 536-537). The Fourth Amendment does not forbid all searches and seizures without a warrant, since there is no constitutional requirement that there must always be judicial authorization before a search or seizure can be made.*

The authority of the government to conduct searches without a warrant in certain situations is well established. Thus, customs agents have the right to search persons and their property at the border and without needing probable cause to believe that they are committing a crime. See *Boyd v. United States*, 116 U.S. 616, 623; *Alexander v. United States*, 362 F. 2d 379 (C.A. 9), certiorari denied, 385 U.S. 977; *United States v. Johnson*, 425 F. 2d 630 (C.A. 9); *Walker v. United States*, 404 F. 2d 900 (C.A. 5). The government similarly may search persons entering government buildings. See *Barrett v. Kunzig*, civ. No. 6193, M.D. Tenn., decided August 11, 1971, *infra*, n. 6. Finally, searches without a warrant have been upheld where, as here (see *infra*, p. 19), they were not related to a criminal investigation. *Abel v. United States*, 362 U.S. 217; see, also *Wyman v. James*, 400

* See, e.g., *Carroll v. United States*, 267 U.S. 132; *McDonald v. United States*, 335 U.S. 451; *Schmerber v. California*, 384 U.S. 757; *Cooper v. California*, 386 U.S. 58; *Warden v. Hayden*, 387 U.S. 294; *Terry v. Ohio*, 392 U.S. 1; *Chimel v. California*, 395 U.S. 752; *Chambers v. Maroney*, 399 U.S. 42; *Wyman v. James*, 400 U.S. 309, 318-324. The seizure of contraband goods under civil process is not subject to the warrant requirement of the Fourth Amendment. *Boyd v. United States*, 116 U.S. 616; *Murray's Lessee v. Hoboken Land and Improvement Co.*, 18 Howard 272. Nor is it required that every search that yields evidence of criminal conduct be supported by a prior warrant. *Abel v. United States*, 362 U.S. 217.

U.S. 309, 318-324. The government's contention that a warrant is not required for the particular type of search in this case accordingly involves no novel principle of constitutional law, but rather the application to these facts of existing doctrine.

Thus, the fact that the surveillance in this case was done without a warrant does not automatically make the search and seizure unreasonable. "[T]he central inquiry under the Fourth Amendment [is] the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security" (*Terry v. Ohio*, 392 U.S. 1, 19).

Furthermore, we think that in balancing the competing interests involved the degree of invasion that the particular search and seizure produces must be taken into account. Cf. *Terry v. Ohio*, *supra*. The overhearing of a telephone conversation—and particularly where, as here, the speaker's own telephone has not been tapped but the overhearing results from his telephone call to a number that is under surveillance (see pp. 30-31, n. 13, *infra*)—involves a lesser invasion of privacy than a physical search of a man's home or his person. While such surveillance is subject to the Fourth Amendment (*Katz v. United States*; *supra*), the determination of its reasonableness properly should take cognizance of the extent of the invasion of privacy involved.

The electronic surveillance in this case was made, as we develop in the next point of this brief, in order to gather intelligence information that the Attorney General, acting on behalf of the President, concluded was necessary to protect the national security. The

governmental interest in this case, therefore, is not merely law enforcement, important as that obviously is, but protection of the fabric of society itself. "Civil liberties, as guaranteed by the Constitution, imply the existence of an organized society maintaining public order without which liberty itself would be lost in the excesses of unrestrained abuses" (*Cox v. New Hampshire*, 312 U.S. 569, 574). Moreover, "[i]n determining whether a particular inspection [or search] is reasonable * * * the need for inspection [or search] must be weighed in terms of these reasonable [governmental] goals * * *" (*Camara v. Municipal Court, supra*, 387 U.S. at 535). Cf. *Anderson v. Sills*, 56 N.J. 210, 226, 229, 265 A.2d 678, 687, 688.

As the Court also pointed out in *Camara*, "[i]n assessing whether the public interest demands creation of a general exception to the Fourth Amendment's warrant requirement, the question is not whether the public interest justifies the type of search in question but whether the authority to search should be evidenced by a warrant, which in turn depends in part upon whether the burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search" (387 U.S. at 533). Though the general rule may be that "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment" (*Katz v. United States, supra*, 389 U.S. at 357), exceptions do exist. See *supra*, p. 12. As we now show, "the governmental purpose behind the search" is a proper one, and that purpose "is likely to [be]

frustrate[d]" by imposing a warrant requirement for surveillance in national security cases (*Camara, supra*, 387 U.S. at 533).

B. When the Governmental Interest in Protecting National Security is Balanced Against the Invasion of Personal Rights Resulting from Electronic Surveillance, the Proper Conclusion is That a Warrant is not Required Before Such Surveillance may be Made.

1. *The President has a duty to protect the national security and he has authority to gather intelligence information necessary to perform that function.*

A fundamental right of any society is to preserve itself and to maintain its government as a functioning and effective organism. Article II, Section 1 of the Constitution vests the executive powers in the President and requires him to preserve, protect and defend the Constitution and the government created by it. As chief executive, the President is responsible for insuring that our system of government functions as a viable entity. Implicit in that duty is protecting the existing system of government against overthrow by unlawful means and assuring that the government can function effectively.

In fulfilling this responsibility, the President must exercise an informed judgment. This in turn requires that all pertinent information be readily available to him. This is particularly important with respect to his obligation to protect the government from unlawful overthrow, since he cannot remain passive until there may be actual acts of insurrection or sabotage. Instead, the President must be able to collect in ad-

vance and on a continuing basis the information he needs to protect the government against destruction or such weakening as renders it impotent to function. This gathering of information is not undertaken for prosecution of criminal acts, but rather to obtain the intelligence data deemed essential to protect the national security. The distinction between the collection of intelligence information to protect the national security and a search made in connection with a criminal investigation has been recognized by Congress in the Omnibus Crime Control and Safe Streets Act of 1968, discussed *infra*, pp. 20-21.

This Court has recognized the President's authority and duty to collect and utilize intelligence information so that he can properly fulfill his constitutional responsibilities.* In *Totten v. United States*, 92 U.S. 105, the Court noted that the President "was undoubtedly authorized during the [civil] war, as commander-in-chief of the armies of the United States, * * * [to] obtain [intelligence] information." It noted further that the nature of that Presidential responsibility required that both the type of intelligence-gathering technique employed and the fact that such technique was being employed not be made public (92 U.S. at 106-107)..

Presidentially-authorized surveillance in national

* See, e.g., *In re Debs*, 158 U.S. 564, *Oetjen v. Central Leather Co.*, 246 U.S. 297; *United States v. Curtiss-Wright Corp.*, 299 U.S. 304, 320-321; *United States v. Belmont*, 301 U.S. 324; *United States v. Pink*, 315 U.S. 203; *Chicago and Southern Air Lines, Inc. v. Waterman Steamship Corp.*, 333 U.S. 103, 111; *Cafeteria Workers v. McElroy*, 367 U.S. 886.

security cases involving threats to overthrow or subvert the government by unlawful means has been undertaken by successive Presidents over a period of thirty years.⁵ In 1940, President Roosevelt notified Attorney General Jackson by confidential memorandum of the necessity to utilize wire-tapping in matters "involving the defense of the nation," and directed him "to authorize the necessary investigation agents that they are at liberty to secure information by listening devices direct to the conversation or other communications of persons suspected of subversive activities against the Government of the United States * * *" (App. 69). Attorney General Clark in 1946 advised President Truman of this earlier directive, and recommended that "in the present troubled period in international affairs, accompanied as it is by an increase in subversive activity here at home, it is as necessary as it was in 1940 to take the investigative measures referred to in President Roosevelt's memorandum. * * * While I am reluctant to suggest any use whatever of these special investigative measures in domestic cases, it seems to me imperative to use them in cases vitally affecting the domestic security. * * *" President Truman explicitly concurred in the recommended policy (App. 70-71). Later Presidents have adhered to this policy (*e.g.*, memorandum from President Johnson acknowledging "that mechanical and electronic [surveillance] devices may some-

⁵ See generally Brownell, *The Public Security and Wire Tapping*, 39 Cornell L. Q. 195, 199-200 (1954); Rogers, *The Case for Wire Tapping*, 63 Yale L.J. 792, 795-796 (1954).

times be essential in protecting our national security" (App. 71)). The exercise of this power for 30 years itself supports its existence, since "in determining the * * * existence of a power, weight shall be given to the usage itself—even when the validity of the practice is the subject of investigation" (*United States v. Midwest Oil Co.*, 236 U.S. 459, 473).

The need for these investigative measures in national security cases continues to the present.⁶ In the last several years the number of acts of sabotage against the government has increased at an alarming rate. The President must protect the government—and thereby the society for whose benefit it exists—and proper performance of this function still requires, as it has in the past, the occasional use of electronic

⁶ In recent years many groups and individuals have threatened to use force and other illegal means to attack and subvert the government and have committed many violent acts to accomplish this end. Because of this, both state and federal officials frequently found it necessary to station guards at entrances to government buildings and to inspect and search packages brought into the buildings. The authority to conduct such inspections and searches without a warrant was recently upheld in *Barrett v. Kunzig*, Civ. No. 6193, M.D. Tenn., decided August 11, 1971.

⁷ See Staff Study of Bombings in the United States, January 1, 1969 through July 1, 1970, Exhibit 825 to the Hearings before the Senate Permanent Subcommittee on Investigations of the Committee on Government Operations on *Riots and Civil and Criminal Disorder*, Part 25, 91st Cong., 2d Sess. (1970). Statistics from the National Bomb Data Center indicate that, in the twelve month period from July 1, 1970, to July 1, 1971, there were 3,285 bombings in the United States, most of which involved government-related facilities. Statistics, National Bomb Data Center, Management and Research Division, International Ass'n of Chiefs of Police (1971).

surveillance to gather information concerning the plans of those who have committed themselves, in many instances publicly, to engage in covert, terrorist tactics to destroy and subvert the government.

2. *The Attorney General, acting on behalf of the President, may authorize surveillance in national security cases.*

a. *In authorizing such surveillance the Attorney General properly acts on behalf of the President.* The President, of course, cannot himself directly do all of the acts involved in the performance of his constitutional functions. Necessarily, he must delegate many of them—particularly those that involve detailed work requiring a large group of experts—to those of his subordinates who are best able to perform the job. The President has given the responsibility to act for him in gathering domestic intelligence information to the government's chief legal officer, the Attorney General.

We stress once again that, in conducting such national security surveillances, the Attorney General is gathering intelligence information for the President, not obtaining evidence for use in criminal prosecution.⁸ As noted above (*supra*, p. 12), there may be less need for a warrant where the purpose of the search is not criminal investigation.

The Attorney General properly acts for the President in this area. It is well settled that "[e]ach head

⁸ That fact distinguishes the present case from *Coolidge v. New Hampshire*, 403 U.S. 443, where the warrant was issued to obtain information for a subsequent criminal prosecution.

of a department is and must be the President's *alter ego* in the matters of that department where the President is required by law to exercise authority." *Myers v. United States*, 272 U.S. 52, 133; *Knauff v. Shaughnessy*, 338 U.S. 537; see, also, *Brownell v. Rasmussen*, 235 F. 2d 527 (C.A.D.C.), certiorari dismissed, 355 U.S. 859. Cf. *Katz v. United States*, 389 U.S. 347, 364 (Mr. Justice White, concurring). Thus, in determining the reasonableness under the Fourth Amendment of national security surveillances made without a warrant, the governmental authority involved is that of the President.

b. *The standard of national security that the Attorney General applies is the same standard Congress provided in the Omnibus Crime Control and Safe Streets Act of 1968.* The standard of the national security that the Attorney General applies in authorizing electronic surveillance without a warrant is the same standard that Congress provided in the Omnibus Crime Control and Safe Streets Act of 1968. In that Act, Congress exempted from the warrant requirements (which it provided for electronic surveillance in connection with criminal investigations) five categories, with respect to which the Act does not limit "the constitutional power of the President to take such measures as he deems necessary to protect" the United States. Three of these categories relate to the hostile acts of a foreign power and to foreign intelligence activities and are not directly involved here. But see *infra*, pp. 30, 34. The two other categories are "to protect the United States against the overthrow

of the Government by force or by other unlawful means, or against any other clear and present danger to the structure or existence of the Government" (18 U.S.C. 2511(3)).

These were the grounds upon which the Attorney General authorized the surveillance in the present case. As his affidavit stated (App. 20), the wiretaps "were being employed to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government."

c. The Attorney General's action in authorizing the surveillance is subject to limited judicial review. We make no contention that the Attorney General's action in concluding that a particular surveillance is necessary to protect the national security is immune from judicial review. Once the surveillance has been made, the courts may review it to determine its conformity with the standard of the Fourth Amendment, just as they review any other search and seizure that is challenged in the criminal proceeding by a motion to suppress or an objection to evidence. Indeed, that was the procedure that the defendants followed in the present case, when shortly after the indictment they moved to compel the government to disclose the information it had obtained through electronic surveillance.

Normally, such judicial review would not take place until a criminal prosecution has been initiated—and, of course, most national security electronic surveillances do not result in prosecutions. The point at

which it would be made—whether at the outset of the proceeding, or later on—lies in the discretion of the trial court.

In determining the validity of the surveillance under the Fourth Amendment standard of reasonableness, the scope of judicial review should be extremely limited. Unless it appears that the Attorney General's determination that the proposed surveillance relates to a national security matter is arbitrary and capricious, *i.e.*, that it constitutes a clear abuse of the broad discretion that the Attorney General has to obtain all information that will be helpful to the President in protecting the government against "overthrow" * * * by force or other unlawful means or against any other clear and present danger to [its] structure or existence" (Omnibus Crime Control and Safe Streets Act of 1968), the court should sustain it. The court should not substitute its judgment for that of the Attorney General on whether the particular organization, person or event involved has a sufficient nexus to protection of the national security to justify the surveillance.

The judgment involved in determining whether to authorize a particular surveillance depends upon such a wide variety of facts and considerations, many of which involve information that necessarily must be kept confidential (see *infra*, pp. 24-26), that the courts rarely would be able to make an informed judgment on the necessity for the particular inquiry. The nature of the gathering of national security intelligence information makes inappropriate any attempt by the

courts to review the need or wisdom for a particular surveillance. The traditional standard of probable cause would be wholly inappropriate for testing the reasonableness under the Fourth Amendment of this category of search and seizure. See *United States v. White*, 401 U.S. 745, 782-783, n. 19 (Mr. Justice Harlan, dissenting).

Moreover, in view of the extremely sensitive nature of the President's actions and decisions in the area of national security and the interrelationship that frequently exists between domestic and foreign intelligence (see *infra*, pp. 24-25, 34), we urge that such judicial review of the legality of the surveillance may "appropriately be made in *ex parte*, *in camera*, proceedings" (*Giordano v. United States*, *supra*, 394 U.S. at 314, Mr. Justice Stewart, concurring)—as the government proposed in the present case. The material considered in such *in camera* proceeding would, of course, be available under the same restriction to the appellate courts. (We also urge, see Point II of the brief, that if surveillance is determined to be illegal, an initial determination of arguable relevance to the prosecution should be made *in camera*.)

3. *The Fourth Amendment Does not Require a Warrant for a National Security Electronic Surveillance That the Attorney General has Authorized.*

a. *Requiring a warrant in national security electronic surveillance is likely to frustrate the governmental purpose of such surveillance.* "[W]hether the authority to search should be evidenced by a warrant * * * depends in part upon whether the burden

of obtaining a warrant is likely to frustrate the governmental purpose behind the search" (*Camara v. Municipal Court*, 387 U.S. 523, 533). Requiring a warrant for electronic surveillance would seriously handicap the ability of the government to obtain vital information relating to national security.

In deciding to use surveillance in such cases, the Attorney General has available and relies upon the entire spectrum of information available to the President. Much of it is derived from sources and involves matters which, by their nature, are highly confidential and must be kept secret. Disclosure to a magistrate of all or even a significant portion of the information and policy considerations the Attorney General weighed in reaching his decision would create serious potential dangers to the national security and to the lives of informants and agents. Without such information, however, the magistrate could not properly perform his traditional function in determining whether the government had a sufficient basis to justify the issuance of a warrant. In order to obtain a warrant, the government would have to show the need for the surveillance by producing information concerning its proposed subject which would entail disclosure of important intelligence information and its sources.

Disclosure of the reasons for a surveillance or even that it is to be conducted could, because of the sensitive nature of the information sought and of most surveillance targets, make an effective surveillance impossible and thus prevent the government from ob-

taining vital information. Secrecy is the essential ingredient in intelligence gathering; requiring prior judicial authorization would create a greater "danger of leaks * * *", because in addition to the judge, you have the clerk, the stenographer and some other officer like a law assistant or bailiff who may be apprised of the nature" of the surveillance. Brownell, *The Public Security and Wire Tapping*, 39 Cornell L. Q. 195, 210 (1954).

Requiring a warrant for national security surveillance would compel the judiciary to embark upon a far different kind of inquiry than courts now make in considering an application for a warrant. In the usual law enforcement situation, the police officer who comes before the magistrate seeking a warrant is able to rely upon a small number of simple facts to indicate probable cause to believe that a crime has been committed at a particular place or by a particular person. In national security surveillance cases, however, the justification for the surveillance ordinarily cannot be simply stated or easily demonstrated; generally it involves a large number of detailed and complicated facts whose interrelation may not be obvious to one who does not have extensive background information, and the drawing of subtle inferences. Moreover, unlike the traditional searches made pursuant to warrants that magistrates issue upon a showing of probable cause, national security surveillances are not designed to obtain facts needed in a criminal investigation, but to obtain intelligence information. Such surveillances involve matters outside the "experience

or facilities" of the judiciary; "[t]he investigative issues do not lie within traditional judicial expertise; they are intrinsically police problems, and should be handled by the executive branch." Telford Taylor, *Two Studies in Constitutional Interpretation*, 89 (1969).

Thus, requiring a warrant frequently would compel the Attorney General to choose between either disclosing to a magistrate highly sensitive information that in the opinion of the government's chief law officer should be kept confidential, or foregoing the use of a proven effective method of gathering intelligence information necessary to the national security.* Whatever course the Attorney General followed in that situation would be inimical to the national interest. The governmental objective here is of grave importance, and the Constitution should not be construed to "withdraw from the Government the power to safeguard its vital interests" in the area. *United States v. Robel*, 389 U.S. 258, 267; see also *Aptheker v. Secretary of State*, 378 U.S. 500, 509.

Permitting the Attorney General to authorize national security surveillance without first obtaining approval of a magistrate would serve the desirable

* See the report of William H. Crouch, Chief, American-British law Division of the Library of Congress, in *Wiretapping, Eavesdropping, and the Bill of Rights*, the Hearings pursuant to S. Res. 234, before the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, 85th Cong., 2d Sess., 137 *et seq.* (1958).

objective of promoting uniformity in the standard governing such surveillances, since a single individual rather than a large number of judges would make the determination.¹⁰ Centralized responsibility also would permit greater control over use of this technique by facilitating close congressional oversight of the Executive's action.¹¹ See Telford Taylor, *supra*, at 90. Great Britain has made the same judgment. In 1957 it rejected a proposal to substitute prior judicial authorization of surveillance for the then existing system of permitting the executive branch, acting alone, to do

¹⁰ The Attorney General personally authorizes each national security surveillance, and does so only when he concludes that the information to be obtained thereby is essential to the protection of the government. One result of this careful and personal review by the Attorney General is that the number of such surveillances is closely limited; indeed, in recent years it has significantly declined. The number of warrantless "national security" telephone surveillances operated by the Federal Bureau of Investigation in the past ten years has decreased: 1960-78; 1961-90; 1962-84; 1963-95; 1964-64; 1965-44; 1966-32; 1967-38; 1968-33; 1969-49; 1970-36. See, e.g., Hearings before a Subcommittee of the Committee on Appropriations of the House of Representatives, 87th Cong., 2d Sess. 345 (January 22, 1962); Hearings before a Subcommittee of the Committee on Appropriations of the House of Representatives, 88th Cong., 1st Sess. 491 (January 29, 1963); Hearings before a Subcommittee of the Committee on Appropriations of the House of Representatives, 91st Cong., 2d Sess. 754 (February 17, 1970).

¹¹ See Brownell, *supra* n. 5, at 211; Rogers, *supra* n. 5, at 798. See also the statement of Attorney General Brownell in *Wiretapping*, Hearings Before Subcommittee No. 5 of the House Committee on the Judiciary on H.R. 762, 867, 4513, 4728, and 5096, 84th Cong., 1st Sess. 51-52 (1955).

so, because the latter method offered better control and greater uniformity.¹²

b. *Congress has recognized the President's authority to authorize national security electronic surveillance without a warrant.* As we have noted (*supra*, pp. 20-21), in the Omnibus Crime Control and Safe Streets Act of 1968 Congress excepted from the requirement that a warrant be obtained for electronic surveillance certain categories of cases dealing with foreign and domestic intelligence and security. It provided that nothing in that Act shall "limit the constitutional power of the President to take such measures as he deems necessary to protect" the country in those areas. The court of appeals viewed this provision as "completely neutral" on the issue of the President's authority to conduct such surveillance (App. 57). We submit, however, that the legislative

¹² In 1957, a committee of three Privy Councillors was appointed to study the Home Secretary's practice of authorizing electronic surveillance, both in ordinary criminal cases and in national security situations. In its report to the Prime Minister and Parliament, the committee discussed alternatives that had been proposed (*Report of the Committee of Privy Councillors Appointed to Inquire Into the Interception of Communications*, paras. 85, 86 (1957)):

It has been urged in some quarters that the authority for the issue of warrants for interception should not be left exclusively in the hands of the Secretary of State. The chief suggested alternatives that have come to our attention are that the Home Secretary should be assisted by an Advisory Committee or that warrants should be issued only on a sworn information before magistrates or a High Court judge. In our opinion, neither of these proposals would improve matters. If a number of magistrates or judges had the power to issue such warrants, the control of the use to which methods of interception can be put would be weaker than under the present system. It might very well prove easier in practice to obtain warrants.

history reflects a Congressional recognition of the existence of that authority.

The Senate Committee Report explained this provision as follows (S. Rept. No. 1097, 90th Cong., 2d Sess. 94 (1968)):

These provisions of the proposed chapter regarding national and internal security thus provide that the contents of any wire or oral communication intercepted by the authority of the President may be received into evidence in any judicial trial or administrative hearing.

* * * The only limitations recognized on this use is that the interceptions be deemed reasonable based on an *ad hoc* judgment taking into consideration all of the facts and circumstances of the individual case, which is but the test of the Constitution itself (*Carroll v. United States*, 267 U.S. 132 (1925)). The possibility that a judicial authorization for the interception could or could not have been obtained under the proposed chapter would only be one factor in such a judgment. No preference should be given to either alternative, since this would tend to limit the very power that this provision recognizes is not to be deemed disturbed.

Congress thus "recognize(d)" that the President's "power" to authorize "interceptions" of "any wire or oral communication" involving "national and internal security"—which the Attorney General exercises on behalf of the President—"is not to be deemed disturbed."

c. *The considerations involved in authorizing national security surveillance are so interrelated to those*

involved in conducting foreign intelligence operations, and the two activities are so interrelated, that it would be inappropriate to impose stricter standards for the former than for the latter. In rejecting the government's contention that the electronic surveillance here involved did not require a warrant, the district court and the court of appeals placed considerable emphasis on their view that this case involves only domestic and not foreign security problems (e.g., App. 30-31, 47, 51, 63-64). Implicit in this analysis is the recognition that a warrant would not be required for surveillance involving foreign intelligence operations—as the Court of Appeals for the Fifth Circuit recently held in *United States v. Clay*, 430 F. 2d 165, certiorari granted and reversed on another issue, 403 U.S. 698, discussed *infra*, pp. 32-33. We think that the suggested distinction is insupportable, both on the facts of this case¹³ and in most (if not all) national

¹³ The defendant, Plamondon, was not the subject of the surveillance in question (App. 35, 74). As shown in the sealed exhibit filed in the district court, the surveillance was directed to a wholly independent organization, of which Plamondon was not a member, on the basis of information available to the Attorney General from other intelligence operations. Plamondon was overheard during conversations with this organization.

We have lodged with the Clerk of this Court for its *in camera* consideration the same exhibit we submitted to the Court of Appeals for the Ninth Circuit in the *Ferguson* case, which involves the same issue as the present case and is now pending on a petition for a writ of certiorari. *Ferguson v. United States*, No. 71-239. That exhibit consists of additional record of conversations overheard during this surveillance.

We think these records demonstrate that any characterization

security cases within the congressionally defined areas of concern. Foreign and domestic intelligence activities are interrelated aspects of the broad function of protecting national security.

This Court has recognized the broad discretion of the President in the conduct of foreign affairs, and the inappropriateness of judicial reconsideration of his decisions in that field, which necessarily rest upon confidential information whose disclosure would be detrimental to the national interest. *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304; *Chicago and Southern Air Lines, Inc. v. Waterman Steamship Corp.*, 333 U.S. 103. In holding in *Waterman* that orders of the Civil Airlines Board awarding overseas airline routes after approval by the President were not subject to judicial review, the Court stated (333 U.S. at 111):

The President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports are not and ought not be published to the world. It would be intolerable that courts, without the relevant information, should review and perhaps nullify actions of the Executive taken on information properly held secret. Nor can courts sit *in camera* in order to be taken into executive confidences. But even if courts could

of the organization in question as "domestic" is unsupportable. For example, over a fourteen month period, 521 telephone calls were made from this installation to foreign and overseas installations and another 431 calls, the contents of which deal with foreign subject matter, were placed to domestic installations.

require full disclosure, the very nature of executive decisions as to foreign policy is political, not judicial. Such decisions are wholly confided by our Constitution to the political departments of the Government, Executive and Legislative. They are delicate, complex, and involve large elements of prophecy. They are and should be undertaken only by those directly responsible to the people whose welfare they advance or imperil. They are decisions of a kind for which the Judiciary has neither aptitude, facilities nor responsibility and which has long been held to belong in the domain of political power not subject to judicial intrusion or inquiry * * *.

Similar considerations recently led the Court of Appeals for the Fifth Circuit to uphold a wiretap (designated as the fifth) that had "been authorized by the Attorney General, for the purpose of obtaining foreign intelligence information" and made without a warrant. *United States v. Clay*, 430 F. 2d 165, 170, reversed on another issue, 403 U. S. 698. The court explained (430 F. 2d at 171):

Determination of this case requires that we balance the rights of the defendant and the national interest. The Attorney General, who acts

* The Court has recognized that judicial review of the President's action is equally inappropriate in other matters committed to his discretion. See, e.g., *Prize Cases*, 2 Black 635; *Oetjen v. Central Leather Co.*, 246 U.S. 297; *Dakota Central Telephone Co. v. South Dakota*, 250 U.S. 163; *United States v. Belmont*, 301 U.S. 324, 328; *United States v. Pink*, 315 U.S. 203; *Johnson v. Eisenrager*, 339 U.S. 763, 789; *United States v. Hogans*, 369 F. 2d 359 (C.A. 2).

here for the President and Commander-in-Chief, has submitted his affidavit that the fifth wiretap was maintained "for the purpose of gathering foreign intelligence information" and the Attorney General opposed disclosure at the hearing because "it would prejudice the national interest to disclose particular facts concerning this surveillance other than to the court." The fifth log was submitted by the Government for an in camera examination by the Court, which has been made both here and in the District Court. The rights of defendant and the national interest have thus been properly safeguarded. Further judicial inquiry would be improper and should not occur. It would be "intolerable that courts, without the relevant information, should review and perhaps nullify actions of the Executive taken on information properly held secret." *Chicago & Southern Air Lines v. Waterman S.S. Corp.*, 333 U. S. 103, 111, 68 S. Ct. 431, 436, 92 L.Ed. 568 (1948). We, therefore, discern no constitutional prohibition against the fifth wiretap.¹⁵

The reasoning that upholds the power of the Attorney General, exercising the power of the President, to authorize electronic surveillance without a warrant for the gathering of foreign intelligence information is equally applicable to domestic national security matters. In both situations the determination to undertake surveillance requires the evaluation of a multitude of subtle and complicated facts and

¹⁵ See also *United States v. O'Baugh*, 304 F. Supp. 767 (D. D.C.); *United States v. Stone*, 305 F. Supp. 75 (D. D.C.); *United States v. Butenko and Ivanov*, No. 418-63, D. N.J., decided October 13, 1970; *United States v. Dellinger, et al.*, Cr. 69-180, N. D. Ill., E.D., decided February 20, 1970.

considerations whose very nature requires that they not be made public, and which are not appropriate for judicial scrutiny. See, *supra*, pp. 24-26.

Moreover, no sharp and clear distinction can be drawn between "foreign" and "domestic" information. The line between them frequently blurs and overlaps, and a surveillance that originally involved foreign intelligence information may quickly extend to domestic activity and vice versa. Organizations that appear to be wholly domestic may in fact have significant foreign ties, as may American nationals connected with such organizations. To attempt to compartmentalize national security into rigid separate segments of "foreign" and "domestic" ignores the realities of the way in which many organizations and individuals whose activity must be kept under surveillance to protect national security operate, and the manner in which intelligence operations must be conducted.

Congress itself has recognized in the Omnibus Crime Control and Safe Streets Act of 1968 that foreign and domestic intelligence activities are overlapping and interrelated. It excepts five general categories of matters from the requirement that a warrant be obtained for electronic surveillance. Three of them relate to foreign intelligence.¹⁶ and two to internal security.

¹⁶ These three categories are (18 U.S.C. 2511(3)):

to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. * * *

d. The possibility that the Attorney General could abuse his power to authorize national security electronic surveillance without a warrant is not a valid reason for denying him that power. The court of appeals was apparently concerned that if the Attorney General has the power to authorize national security electronic surveillance without a warrant, he could abuse that power (App. 60-61). But any power that a government official possesses is subject to abuse, and that possibility is not a valid reason to deny him the power.

The Attorney General's determination to authorize surveillance is, as we recognize (*supra*, pp. 21-23), subject to judicial review, although of limited scope. If the Attorney General should ever abuse his authority in authorizing a surveillance, i.e., if the subject of surveillance bore no reasonable relation to national security, the courts could correct the situation. The possibility of such an abuse, however, is not a valid basis for denying the Attorney General the authority.

II

IF IT IS DETERMINED THAT ELECTRONIC SURVEILLANCE TO PROTECT NATIONAL SECURITY IS UNLAWFUL IN THE ABSENCE OF PRIOR JUDICIAL AUTHORIZATION, COURTS SHOULD BE PERMITTED TO DETERMINE IN CAMERA WHETHER ILLEGAL INTERCEPTIONS ARE ARGUABLY RELEVANT TO A PROSECUTION BEFORE REQUIRING THEIR DISCLOSURE TO THE DEFENDANT

If this Court should conclude, contrary to the position urged in Point I of this brief, that electronic surveillance to protect the national security requires

prior judicial authorization, then we urge that it reconsider *Alderman v. United States*, 394 U.S. 165, and hold that the requirement of automatic disclosure of interceptions to defendants announced in that case is inapplicable to this kind of surveillance. When interceptions are made for national security purposes, the reasons are especially strong for permitting courts to determine *in camera* whether the information obtained thereby is arguably relevant to a prosecution before turning the material over to a defendant; and courts should be permitted to make an initial determination *in camera* with respect to these interceptions.

We recognize that *Alderman* appears to require automatic disclosure for every circumstance in which there is an unlawful interception of a defendant's voice, but reconsideration is appropriate in this context for a number of reasons. The majority opinion in that case does not state that the issue of automatic disclosure versus an initial *in camera* proceeding can be decided by easy reference to some constitutional text. Rather, it rests on the premise that the issue must be determined on the basis of a balancing of the defendant's interest in adequate protection of his rights against the reasons for not disclosing material that does not appear arguably relevant. Subsequent to *Alderman* this Court held that *in camera* proceedings were appropriate for the identification of intercepted voices and stated that "[n]othing in *Aldermen v. United States* [and its companion cases] * * * requires an adversary proceeding and full disclosure for resolution of every issue raised by an electronic sur-

veillance." *Taglianetti v. United States*, 394 U.S. 316, 317. And amplifying on the *per curiam* disposition in *Giordano v. United States*, 394 U.S. 310, Mr. Justice Stewart noted that the Court had not decided that an *in camera* proceeding was inappropriate for the determination of whether surveillance was legal or not. *Id.*, at 314. Since nondisclosure has been found acceptable in other contexts, see, e.g., *Alderman*, *supra*, 394 U.S. at 182-183, n. 14; *Roviaro v. United States*, 353 U.S. 53, there is no absolute constitutional rule of disclosure of every bit of information that might conceivably be of interest to a defendant, and it is proper for the Court to consider now whether automatic disclosure is required for national security interceptions.

Moreover, the opinion in *Alderman* does not make clear whether the Court imposed the rule of that case as a constitutional requirement or under its supervisory power to regulate admission of evidence in the federal courts. We believe that the case reflects an exercise of the supervisory power. Since Congress, in the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2518(8)(d) and (10)(a), has taken a more flexible approach to disclosure than *Alderman*, that decision may well be superseded by legislation with respect to post-1968 surveillance. The legislative history of Title VII of the Organized Crime Control Act of 1970, 84 Stat. 935, 18 U.S.C. 3504, reflects the view of Congress that *Alderman* imposes a rule that is too inflexible. Even if *Alderman* is thought to be of constitutional dimension, this considered legislative judgment should be given weight in the decision

whether to require automatic disclosure for national security interceptions.

1. Whether there should be a rule of automatic disclosure of interceptions, rather than a preliminary *in camera* review for arguable relevance, is not an easy question, even in the context of ordinary criminal cases. Disclosure of overheard conversations has a serious potential for injury to persons who have completely innocent conversations with those who are subsequently prosecuted and receive the disclosure, and even to persons who are not a party to any overheard conversations but may be referred to in those conversations.¹⁷ In some circumstances, the lives and families of government informants may be endangered. Pending investigations and prosecutions can be significantly impaired by the mere disclosure of their existence, which frequently leads to flight by potential defendants and destruction of important evidence. Where the pending matters involve state proceedings

¹⁷ See e.g., *Life Magazine*, May 30, 1969, pp. 45-47. Excerpts from transcripts of conversations overheard through government electronic surveillances published there contained unflattering references to prominent entertainment figures, elected officials, and members of the judiciary, none of whom was a party to any of the published conversations. While a protective order under Rule 16(e) of the Federal Rules of Criminal Procedure might reduce this risk, the fact is that such orders have not been uniformly successful. Here, too, the more people who are shown the material, the greater the danger of exposure, unwitting or purposeful. See Reply Memorandum for the United States, *Kolod, et al. v. United States*, No. 133, O.T. 1967 (March 1968), at p. 4; Memorandum for the United States, *Kolod et al. v. United States*, No. 133, O.T. 1967 (April 1968), at pp. 6-7, 16-22.

as well, these undesirable side effects also impinge on state interests and may strain the needed cooperative relationships between federal and state law enforcement agencies.

All these problems are compounded in national security cases, where intelligence gathering is the objective and secrecy is absolutely necessary. Disclosure often will include information pinpointing the location of a particular listening device, information which may be extremely damaging in national security cases. Or the disclosure may reveal the existence of an independent source of information, or the identity of a government secret agent. The very nature of the operations involved in this area frequently militates strongly against the government disclosing its activities, if it is not to compromise the national security. Automatic disclosure here thus operates against the public interest in the government's not revealing generally its intelligence-gathering operations, because such disclosure "might compromise or embarrass our government in its public duties." *Totten v. United States*, *supra*, 92 U.S. at 106; see also *United States v. Reynolds*, 345 U.S. 1.

The argument against automatic disclosure is particularly strong in a case like this one, in which a person who is or becomes a defendant in a criminal case is overheard merely by happenstance. The individual overheard is not himself the subject of surveillance, but his conversation is intercepted incidentally and wholly irrelevantly (in respect to his prosecution), in connection with a surveillance to obtain in-

telligence information to protect the national security.¹⁸ In this situation, the contention that an *in camera* proceeding will inadequately protect the defendant is singularly weak, since the judge can determine without great difficulty that an interception bears no relation to a prosecution.

If disclosure is required in this area, the government must face the dilemma of either dropping the prosecution of an often serious criminal offense or revealing sensitive national security information. When the latter course cannot be followed, the result of the automatic disclosure rule, in practical terms, is to provide the defendant with immunity from prosecution for all crimes, past, present, or future; it may even encourage defendants and potential defendants to telephone persons or locations that they suspect may be the subject of surveillance. This undesirable result can be avoided if disclosure may first be made to the court alone, without further disclosure if the court finds that the material is not arguably relevant to the prosecution.

2. The majority opinion in *Alderman* does not specifically indicate whether the rule of that case rests on the Court's supervisory power over the admission of evidence in federal courts or on the Constitution, but most reasonably that decision may be viewed as an exercise of the supervisory power. Congress, of

¹⁸ In this case, the defendant, Plamondon, was not the subject of the surveillance authorized by the Attorney General. He was overheard when, fortuitously, he made a call to the telephone installation which was the subject of the surveillance. See pp. 30-31, n. 13, *supra*.

course, has the power to supersede nonconstitutional decisions. Electronic surveillance in ordinary criminal investigation is now regulated by provisions, 18 U.S.C. 2510-2520, adopted in 1968 as part of the Omnibus Crime Control and Safe Streets Act of 1968. When a person who is prosecuted believes he has been the subject of illegal surveillance, he may move to suppress the contents of intercepted communications and evidence derived therefrom. If such a motion is filed the judge "may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice." 18 U.S.C. 2518(10) (a)(iii); see also 18 U.S.C. 2518(8)(d). The statute, thus, does not adopt an automatic disclosure rule, but gives the judge discretion to determine if disclosure is in the interests of justice.¹⁹ We contend that this provision supplants the rule of *Alderman* in the circumstances to which the statute applies.

In 18 U.S.C. 2511(3), discussed *supra*, Congress excepted national security surveillance from the reach of the 1968 Act because it intended the govern-

¹⁹ According to the committee report (S. Rep. No. 1097, 90th Cong., 2d Sess. 106 (1968)):

This provision explicitly recognizes the propriety of limiting access to intercepted communications or evidence derived therefrom according to the exigencies of the situation. The motion to suppress [evidence] envisioned by this paragraph should not be turned into a bill of discovery by the defendant in order that he may learn everything in the confidential files of the law enforcement agency. Nor should the privacy of other people be unduly invaded in the process of litigating the propriety of the interception of an aggrieved person's communications.

ment to be able to operate in that area without the stringent limitations that the Act imposed. If, contrary to the congressional view and our submission in Point I above, such surveillance is subjected to pre-overhearing judicial scrutiny, then Congress would certainly intend that the requirement to disclose information gathered be no greater than in the ordinary criminal situation. It is clear that Congress would not want a rule of automatic disclosure for national security cases when it has not provided such a rule in ordinary cases. Thus, if *Alderman* does rest on the supervisory power, as we urge, it should be considered superseded for interceptions occurring, as this one did, after enactment of the 1968 legislation.

3. In Title VII of the Organized Crime Control Act of 1970, 84 Stat. 935, 18 U.S.C. 3504, Congress provided that

2) disclosure of information for a determination if evidence is inadmissible because it is the primary product of an unlawful act occurring prior to June 19, 1967,²⁰ or because it was obtained by the exploitation of an unlawful act occurring prior to June 19, 1968, shall not be required unless such information may be relevant to a pending claim of such inadmissibility

* * *

This statute is not applicable to the overhearing involved here, which occurred after June 1968. But its passage and legislative history are significant. The leg-

²⁰ As passed, in Pub. Law 91-452, October 15, 1970, this date reads June 19, 1968.

islative history indicates that this subsection rejects the approach of *Alderman* and is designed to establish a procedure like that argued for by the government in that case. It further indicates the congressional view that *Alderman* is based on the supervisory power rather than a constitutional mandate and is, thus, subject to legislative change. Interceptions occurring after June 19, 1968, were not covered by this enactment only because it was assumed that these were covered by the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510, *et seq.*, rather than *Alderman*. Finally, the legislative history reflects a determination that protective orders intended to restrict dissemination of matters turned over to the defense ~~pursuant to the defense~~ pursuant to the *Alderman* requirement are ineffective to preserve the secrecy of interceptions.

The Senate Report, No. 91-617, 91st Cong., 2d Sess. 64 (1970) states that "[b]ecause the price of requiring such admittedly indiscriminate disclosure is so inordinately high, the *Alderman* decision must be set aside by congressional action." As an example of the inefficacy of protective orders, the Report, *id.* at 69, noted:

National security information dealing with surveillance of a foreign embassy was disclosed in a December 2, 1966; Washington Post article in spite of a protective order made by the Federal District Court for the District of Columbia. Again, the wiretap transcripts had remained confidential in the Government's hands for over 5 years until they were produced in

court, supposedly in secret, only to appear in the newspaper 3 weeks later.²¹

During the House debate on the Senate's Title VII proposal, Congressman Poff, a member of the House Committee on the Judiciary who explained the provisions of the 1970 Act on the floor of the House, stated (116 Cong. Rec. H9649 (daily ed. Oct. 6, 1970)):

Next, my colleagues turn to title VII of S. 30, which would, first, reverse the Supreme Court's decision in *Alderman v. United States*, 394 U.S. 165 (1969) requiring, under its supervisory power, the disclosure of Government files in criminal trials * * *.²²

He later elaborated on the scope of the 1970 provisions (116 Cong. Rec. H9710-9711 (daily ed. Oct. 7, 1970)):

Where there was in fact an unlawful overhearing prior to June 19, 1968, the title provides for

²¹ Another example involves the so-called Patriarca transcripts in the *Taglianetti* case (see 394 U.S. 316) which, despite a protective order, were made available to a newspaper reporter by court clerks and thereafter widely disseminated. See Richard Connolly, *The Story of the Patriarca Transcripts*, Boston Evening Globe, September 2, 1971, p. 22, cols. 3-6.

²² Numerous other Senators and Congressmen expressed their displeasure with the automatic disclosure rule of *Alderman*. See, e.g., Senator McClellan, at 115 Cong. Rec. S5810-5816 (daily ed. May 29, 1969); *id.* at S6092-6096 (daily ed. June 9, 1969); 116 Cong. Rec. S127-130 (daily ed. Jan. 19, 1970); *id.* at S334-335 (daily ed. Jan. 21, 1970); Senator Hruska, at 116 Cong. Rec. S464-471 (daily ed. Jan. 23, 1970); Congressman McCulloch, at 116 Cong. Rec. H9655 (daily ed. Oct. 6, 1970); Congressman Railsback, at 116 Cong. Rec. H9721 (daily ed. Oct. 7, 1970); and Congressman Minish, at 116 Cong. Rec. H9730 (daily ed. Oct. 7, 1970).

an *in camera* examination of the Government's transcripts and records to determine whether they may be relevant to the claim of inadmissibility. Where there is no relevancy whatsoever, as determined by the Court, the transcripts need not be disclosed to the claimant or his counsel. To require disclosure under such circumstances can serve no purpose in the interest of justice, and may needlessly jeopardize the lives of Government agents and informants, harm the reputation of innocent third persons, and compromise the national security. To the extent that the court is permitted to determine relevancy in an *ex parte* proceeding, the title will modify the procedure established by the Supreme Court in *Alderman v. United States*, 394 U.S. 165 (1968). The Court in *Alderman* assumed that adequate protection against the dangers inherent in disclosure of the Government's records to the defendant and his counsel could be afforded by the use of protective orders, but the experience of the Department of Justice has indicated time and again that protective orders are inadequate even to prevent the unauthorized publication of its records and transcripts in the news media.

As I have indicated, the title applies only to disclosures where the electronic surveillance occurred prior to June 18, 1968. It is not necessary that it apply to disclosure where an electronic surveillance occurred after that date, because such disclosure will be mandated, not by *Alderman*, but by section 2518 of title 18, United States Code, added by title III of the Omnibus Crime Control and Safe Streets Act

of 1968. * * * The provisions of this title will, therefore, control the disclosure of transcripts of electronic surveillances conducted prior to June 19, 1968. Thereafter, existing statutory law, not *Alderman*, will control. * * *

Senator McClellan, who had issued the report on the original Senate bill for the Committee on the Judiciary, agreed that the 1968 Act covered post-1968 interceptions and indicated that its provisions for disclosure coincided with those of the 1970 Act (116 Cong. Rec. S17775 (daily ed. Oct. 12, 1970)):

The House has modified it [Title VII] by making it applicable only to electronic surveillance. Also, it is limited to surveillance that occurred prior to June 1968, the date on which title III of Public Law 90-351 [Omnibus Crime Control and Safe Streets Act of 1968] was enacted.

Electronic surveillance subsequent to that time is controlled by the 1968 [Omnibus Crime Control and Safe Streets] act, where the disclosure standard is the same as it was set out in title VII. See Senate Report No. 1097, 90th Congress, Second Session at 106 (1968). When the Senate passed title VII, it was not limited to electronic surveillance, so it was necessary to make it apply to acts occurring after 1968. This new language applies, however, only to surveillance prior to 1968.

In light of the provisions and history of the 1968 and 1970 Acts, we submit that the automatic disclosure dictated by *Alderman* should be considered superseded by congressional enactment even in respect to ordinary criminal cases. *A fortiori* it was Congress' intent that automatic disclosure not be required in the narrow

class of national security cases which it has exempted from the coverage of the 1968 Act. Even if *Alderman* be regarded as based in part on the Constitution, the special dangers of automatic disclosure for national security interceptions, the inefficacy of protective orders, and the strongly expressed congressional view that initial *in camera* determinations are consistent with the Constitution, should lead this Court not to compel automatic disclosure when interceptions without prior judicial authorization are made to protect the national security.

CONCLUSION

The judgment of the court of appeals should be reversed, and the case should be remanded to that court for further proceedings consistent with the opinion of this Court.

Respectfully submitted.

ERWIN N. GRISWOLD,
Solicitor General.

ROBERT C. MARDIAN,
Assistant Attorney General.

DANIEL J. MCAULIFFE,

ROBERT L. KEUCH,

GEORGE W. CALHOUN,

Attorneys.

SEPTEMBER 1971.

APPENDIX

The Fourth Amendment provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause; supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Omnibus Crime Control and Safe Streets Act of 1968 provides, in pertinent part (82 Stat. 214, 18 U.S.C. 2511(3)):

Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1103, 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.